



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,989	08/22/2003	William E. Sobel	20423-08016	8643

34415 7590 03/14/2008
SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER

KIM, PAUL

ART UNIT	PAPER NUMBER
----------	--------------

2161

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

03/14/2008

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

DETAILED ACTION

1. This Office action is responsive to the following communication: Amendment filed on 13 December 2007.
2. Claims 1-21 and 24-28 are pending and present for examination. Claims 1, 9, and 16 are in independent form.

Response to Amendment

3. Claim 22 has been cancelled.
4. Claim 28 has been added.
5. Claims 1-5, 8-13, 16-20, and 24-27 have been amended.

Claim Rejections - 35 USC § 112

6. As per the rejections under 35 U.S.C. 112, Applicant's amendment has been acknowledged. Accordingly, the rejections have been withdrawn.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.
8. **Claims 16-22 and 24-27** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed toward "a computer system" comprised of a plurality of modules which are only "configured" to perform certain functions. That is, while the modules may be configured to perform said functions, the claim limitations, as recited, would read upon software modules which lack any integrated hardware execution. Accordingly, wherein the claims may read upon software modules, said claims would constitute software, per se. Therefore, the claims fail to

Art Unit: 2161

provide a "useful, concrete and tangible result." See State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. MPEP 2106. "The claimed invention as a whole must accomplish a practical application. That is, it must produce a 'useful, concrete and tangible result'" (emphasis added).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. **Claims 1-3, 6, 8-11, 14, 16-18, 21, and 24-28** are rejected under 35 U.S.C. 103(a) as being unpatentable over Pisello et al (U.S. Patent No. 5,495,607, hereinafter referred to PISELLO), filed on November 15, 1993, and issued on February 27, 1996, in view of Stupek, Jr. et al (U.S. Patent No. 5,586,304, hereinafter referred to as STUPEK), filed on 8 September 1994, and issued on 17 December 1996.

11. **As per independent claim 1, 9 and 16**, PISELLO, in combination with STUPEK, discloses:

A computer implemented method for gleaning file attributes independently of file format, the method comprising the steps of:

a non-application-specific file attribute manager receiving a plurality of files in a plurality of formats {See PISELLO, col. 13, lines 14-19, wherein this reads over "a domain-wide status-monitor . . . periodically scan[s]"};

the file attribute manager scanning the plurality of received files in the plurality of formats {See PISELLO, col. 13, lines 14-19, wherein this reads over "a domain-wide status-monitor . . . periodically scan[s]"};

the file attribute manager gleaning attributes from each of the plurality of scanned files in the plurality of formats {See PISELLO, col. 13, lines 48-51, wherein this reads over "to collect the file identifying information stored at a given scan time"; and col. 15, lines 36-51, wherein this reads over, searchable database fields preferably include: . . . FileName;PathName"};

the file attribute manager storing the file attributes gleaned from each of the plurality of scanned files as a plurality of records in a database {See PISELLO, col. 13, lines 51-56, wherein this reads over "to integrate the collected information into the domain-wide virtual catalog"};

Art Unit: 2161

the file attribute manager indexing specific file attributes gleaned from specific files according to contents of the specific files, the specific file attributes being stored as ones of the plurality of records in the database {See PISELLO, col. 14, lines 16-19, wherein this reads over "Table 2 which shows an example of what might be displayed . . . [from] the domain administrating data/rule base"};

examining one of the plurality of files {See PISELLO, col. 13, lines 14-19, wherein this reads over "a domain-wide status-monitor . . . periodically scan[s]"; and col. 13, lines 48-51, wherein this reads over "to collect the file identifying information stored at a given scan time"; and col. 15, lines 36-51, wherein this reads over, searchable database fields preferably include: . . . FileName;PathName"};

retrieving from the plurality of records in the database at least one record associated with the examined one of the plurality of files {See STUPEK, C3:L64-67, wherein this reads over "the upgrade advisor retrieves information about the MIB 5 from a server database 13 located in the server manager"; and C4:L2-26, wherein this reads over "the upgrade database may also contain information about a resource (e.g., a driver) which is not recognized by the server manager. In this situation, the upgrade advisor places information about the resource (e.g., name, version number) into a driver table 32 in the MIB 5. An agent 21 of the server manager located in the server uses this information to search for the resource (i.e., to see if the resource has been installed on the network). If so, the server manager creates entries for the resource in the server database"};

analyzing the gleaned attributes gleaned from examined one of the plurality of files, the gleaned file attributes having been retrieved from the at least one record associated with the examined one of the plurality of files {See STUPEK, C4:L5-13, wherein this reads over "the upgrade advisor 11 retrieves information about the MIB 5 from a server database 13 located in the server manager. The server database 13 tells the upgrade advisor 11 the location of each piece of information contained in the MIB. The upgrade advisor 11 supplies the location information to a data retriever 15, which uses it to retrieve from the MIB 5 data (MIB data) about the network resources 3. The upgrade advisor 11 then retrieves upgrade information from the upgrade database 9 and performs two types of comparisons: a) whether or not a particular upgrade package corresponds to a resource on the server, and b) whether or not the version number of the upgrade package matches the version number of the corresponding network resource (i.e, whether or not the upgrade package represents a true upgrade for the existing network resource)"}; and

determining a status of the examined one of the plurality of files responsive to analyzing the gleaned file attributes {See STUPEK, C13-20, wherein this reads over "If the upgrade applies to a resource on the server and if the upgraded and current versions of the network resource do not match, the upgrade advisor 11 uses additional information from the upgrade database 9 to analyze the level of severity of the upgrade, i.e., to determine the importance of the upgrade to the efficient operation of the server."}.

While PISELLO fails to expressly disclose the method step of analyzing gleaned attributes and thereafter determining a status, the prior art of STUPEK discloses a method wherein information is retrieved from a database, and said information is summarily compared with upgrade information to determine whether an upgrade is necessary. That is the prior art of STUPEK discloses a method wherein file attributes such as the name, version number, and a timestamp, which have been gleaned from a file, are compared and verified. The combination of inventions disclosed in PISELLO and STUPEK would disclose a method comprising of examining a file, analyzing the gleaned attributes concerning the file

Art Unit: 2161

with records retrieved from the database (e.g. upgrade information), and determining the status of the file (i.e. whether or not the versions match). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by STUPEK.

One of ordinary skill in the art would have been motivated to do this modification so malicious or illegitimate files are blocked from entering the computer, from executing, and from performing certain functions while executing.

12. As per dependent claims 2, 10, and 17, PISELLO, in combination with STUPEK, discloses:

A method wherein specific types of file attributes are gleaned from a specific file as a function of a protocol according to which the file is transmitted {See PISELLO, Table 2, wherein this includes the file-server name under the column labeled "File_Source" and the sender name under the column labeled "By"}.

13. As per dependent claim 3, 11, 18, PISELLO, in combination with STUPEK, discloses:

A method wherein specific types of file attributes are gleaned from a specific file as a function of a format of the file {See PISELLO, col. 15, lines 46-51, wherein this reads over "Novell-defined attributes"}.

14. As per dependent claims 6, 14, 21, PISELLO, in combination with STUPEK, discloses:

A method further comprising the file attribute manager receiving a plurality of copies of a selected file of the plurality of files, and the file attribute manager storing each of the plurality of copies as a separate record in the plurality of records, each separate record indexed according to the contents of the selected file of the plurality of files, such that the each separate record can be accessed by the single index {See PISELLO, Table 2; and col. 14, lines 62-64, wherein this reads over "the same file name may appear multiple times in the listing of Table 2, even with identical path names (e.g., 'Dave.doc')"}.

15. As per dependent claim 8, PISELLO, in combination with STUPEK, discloses:

The method wherein the non-application-specific file attribute manager is incorporated into one selected from the group consisting of:

- A firewall;
- An intrusion detection system;
- An intrusion detection system application proxy;
- A router;
- A switch;
- A standalone proxy;

A server; {See PISELLO, col. 13, lines 14-15, wherein this reads over "domain-wide status-monitor and control program is installed in the domain administrating server"}.

- A gateway

Art Unit: 2161

An anti-virus detection system; and
A client.

Additionally, the claim limitation optionally recites a method wherein the attribute manager is incorporated into an selected entity. for the purposes of this examination, a server will be considered the selected entity and the remainder entities will not be provided further consideration nor will prior art be applied in said consideration.

16. **As per dependent claim 24**, PISELLO, in combination with STUPEK, discloses a method of blocking a file upon the determination that the received file is malicious {See STUPEK, C8:L30-48}.

While PISELLO fails to expressly disclose a method wherein a file is blocked upon a maliciousness determination, STUPEK discloses a method wherein if an upgrade is not applicative, the upgrade is not included within the upgrade package. The combination of inventions disclosed in PISELLO and STUPEK would disclose a method comprising of blocking the file upon the determination that the received file is malicious (i.e. the package object retrieves comparison results and combined them to determine package status (i.e., whether or not the package applies to the server, and whether the package needs to be upgraded on the server). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by STUPEK.

One of ordinary skill in the art would have been motivated to do this modification such that files which are not legitimate are blocked from entering the server, from executing, and from performing certain functions while executing.

17. **As per dependent claim 25**, PISELLO, in combination with STUPEK, discloses a method of not blocking the file upon the determination that the received file is legitimate {See STUPEK, C8:L30-48}.

While PISELLO fails to expressly disclose a method wherein a file is blocked upon a maliciousness determination, STUPEK discloses a method wherein if an upgrade is applicative, the upgrade is included within the upgrade package. The combination of inventions disclosed in PISELLO and STUPEK would disclose a method comprising of allowing the file upon the determination that the received file is

Art Unit: 2161

legitimate (i.e. the package object retrieves comparison results and combined them to determine package status (i.e., whether or not the package applies to the server, and whether the package needs to be upgraded on the server). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by STUPEK.

One of ordinary skill in the art would have been motivated to do this modification such that files which are not legitimate are allowed to enter the server, execute, and perform certain functions while executing.

18. **As per dependent claim 26**, PISELLO, in combination with STUPEK, discloses a method for applying a rule specifying how to use gleaned file attributes to process the file {See STUPEK, C13-20, wherein this reads over "If the upgrade applies to a resource on the server and if the upgraded and current versions of the network resource do not match, the upgrade advisor 11 uses additional information from the upgrade database 9 to analyze the level of severity of the upgrade, i.e., to determine the importance of the upgrade to the efficient operation of the server."}.

The combination of inventions disclosed in PISELLO and STUPEK would disclose a method comprising for applying a rule specifying how to use gleaned file attributes to process a file. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by STUPEK.

One of ordinary skill in the art would have been motivated to do this modification in order to determine the legitimacy of a file by analyzing and processing the gleaned attributes according to a set rule.

19. **As per dependent claim 27**, PISELLO, in combination with STUPEK, discloses a method for determining a rule to apply specifying how to use gleaned file attributes to process the file {See STUPEK, C13-20, wherein this reads over "If the upgrade applies to a resource on the server and if the upgraded and current versions of the network resource do not match, the upgrade advisor 11 uses additional information from the upgrade database 9 to analyze the level of severity of the upgrade, i.e., to determine the importance of the upgrade to the efficient operation of the server."}.

While PISELLO fails to expressly disclose a method for determining a rule to apply specifying how to use gleaned file attributes to process the file, the prior art of STUPEK discloses a method wherein the upgrade manager performs comparisons on the attributes of the file, specifically the version number. The combination of inventions disclosed in PISELLO and STUPEK would disclose a method comprising of determining at least one of a plurality of rules to apply to a file. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by STUPEK.

One of ordinary skill in the art would have been motivated to do this modification so that upon the failure or passage of a file in a rule, further gleaned attributes may be checked to determine the legitimacy of a file.

20. **As per dependent claim 8**, PISELLO, in combination with STUPEK, discloses:

The method of claim 1, wherein the plurality of files are received from a network connection {See STUPEK, Figures 1, 2, 6, and 11}.

21. **Claims 4, 12, and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over PISELLO, in view of STUPEK, and in further view of Fischer (U.S. Patent No. 5,694, 569, hereinafter referred to as FISCHER), filed on June 5, 1995, and issued on December 2, 1997.

PISELLO and STUPEK disclose the limitations of claims 1-3, 6, 8-11, 14, 16-18, and 21 for the reasons stated above.

PISELLO and STUPEK differ from the claimed invention in that they fail to disclose a method further comprising the file attribute manager indexing attributes being stored by using a secure hash of the contents of that file (claims 4, 12, and 19).

22. **As per dependent claim 4, 12, and 19**, PISELLO, in combination with STUPEK and FISCHER, discloses a method further comprising the file attribute manager indexing attributes being stored as a record in the database concerning a specific file according to a secure hash of the contents of that file {See FISCHER, col. 1, lines 40-50, wherein this reads over "file integrity may be protected by taking a one-way hash over the contents of the file. By implementing and checking a currently computed hash value, with a previously stored hash value"}.

Art Unit: 2161

The combination of inventions disclosed in PISELLO, STUPEK, and FISCHER would disclose a method wherein the file attribute manager would index attributes in a database according to a secure hash, by using a secure hash algorithm (SHA), of the contents of that file. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by STUPEK and FISCHER.

One of ordinary skill in the art would have been motivated to do this modification so that the records may be indexed securely and subsequently retrieved by a blocking system.

23. **Claims 5, 13, and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over PISELLO, in view STUPEK, and in further view of Baker (USPGPUB No. 2003/0233352, hereinafter referred to as BAKER), filed on March 19, 2003, claiming priority to March 21, 2002, and published on December 18, 2003.

PISELLO and STUPEK disclose the limitations of claims 1-3, 6, 8-11, 14, 16-18, and 21 for the reasons stated above.

PISELLO and STUPEK differ from the claimed invention in that they fail to disclose a method further comprising the file attribute manager indexing attributes according to a cyclical redundancy check of the contents of that file (claims 5, 13, and 20).

24. **As per dependent claims 5, 13, and 20**, PISELLO, in combination with STUPEK and BAKER, discloses a method further comprising the file attribute manager indexing attributes being stored as a record in the database concerning a specific file according to a cyclical redundancy check of the contents of that file {See BAKER, Para. 0008, wherein this reads over "[t]he controller may be further programmed . . . to determine a cyclical redundancy check of the file"}.

While PISELLO fails to expressly disclose a method of utilizing a CRC on the contents of a file, BAKER discloses a means for applying a CRC on the file for validation purposes. The combination of inventions disclosed in PISELLO, STUPEK, and BAKER would disclose a method wherein the file attribute manager would index attributes in a database according to a cyclical redundancy check of the contents of that file. Therefore, it would have been obvious to one of ordinary skill in the art at the time the

Art Unit: 2161

invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by STUPEK and BAKER.

One of ordinary skill in the art would have been motivated to do this modification so that the records may be indexed securely and subsequently retrieved by a blocking system.

25. **Claims 7, 15, and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over PISELLO, in view of STUPEK, and in further view of Chino et al (USPGPUB 2002/0046207), filed on June 25, 2001, and published on April 18, 2002.

PISELLO and STUPEK disclose the limitations of claims 1-3, 6, 8-11, 14, 16-18, and 21 for the reasons stated above.

PISELLO and STUPEK differ from the claimed invention in that they fail to disclose a method which deletes records from the database after the records have been stored for a specific period of time (claims 7, 15, and 22).

26. **As per dependent claims 7, 15, and 22**, PISELLO, in combination with STUPEK and CHINO, discloses a method further comprising of deleting records from the database after the records have been stored for a specific period of time {See CHINO, Para. 0060, wherein this reads over "location information collector determines whether a predetermined time , e.g. two hours, has passed wince the record of the current location registered in the respective tables of the location information storage was collected, and sequentially deletes those records with a predetermined time elapsed"}.

While PISELLO fails to expressly disclose a method of purging files, CHINO discloses a method of purging records when a predetermined time has elapsed. The combination of inventions disclosed in PISELLO, STUPEK, and CHINO would disclose a method comprising of deleting records with a predetermined time elapsed. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by STUPEK and CHINO.

One of ordinary skill in the art would have been motivated to do this modification so that the database is kept current and free of obsolete records.

Response to Arguments

27. Applicant's arguments filed 13 December 2007, with respect to Pisello and Stupek, as applied to claims 1, 9, and 16, have been fully considered but are not persuasive.

a. Rejections under 35 U.S.C. 103

Applicant asserts the argument that "Stupek, however, neither teaches nor suggests the claimed analyzing and determining steps" (Amendment, page 10). The Examiner respectfully disagrees. It is noted that Stupek discloses a system that "retrieves upgrade information from the upgrade database 9 and performs two types of comparisons." See Stupek, col. 4, lines 5-13. Wherein the upgrade information may consist of a "name" and/or a "version number," said upgrade information would read upon the claimed "file attributes." See Stupek, col. 4, lines 20-26. While Applicant asserts the argument that "Stupek thus utilizes attributes of software, and not attributes of files," the Examiner notes that wherein software is inherently comprised of one or more files, the gleaning of information from the software would inherently result in the gleaning of information from a file. Additionally, it is noted that Applicant's claimed invention only requires that file attributes be gleaned from "the examined one of the plurality of files." Accordingly, one of ordinary skill in the art would have indeed found the claimed invention obvious in view of Pisello and Stupek.

For the aforementioned reasons above, Applicant's arguments with respect to Pisello and Stupek are not persuasive.

Conclusion

28. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2161

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to PAUL KIM whose telephone number is (571)272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Apu Mofiz can be reached on (571) 272-4080. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Apu M Mofiz/
Supervisory Patent Examiner, Art Unit 2161

Paul Kim
Patent Examiner, Art Unit 2161
TECH Center 2100

<div>Application Number</div> <div></div>	Application/Control No.	Applicant(s)/Patent under Reexamination	
	10/645,989	SOBEL, WILLIAM E.	
	Examiner	Art Unit	
	PAUL KIM	2161	